Department of Homeland Security Daily Open Source Infrastructure Report for 12 December 2005

Current Nationwide Threat Level is ELEVATED — Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports six people were arrested in Oregon, Arizona, Virginia, and New York on ecoterrorism charges in an FBI sweep on both coasts. (See item 1)
- BusinessWeek reports law enforcement officials say prepaid gift cards, many of which can be reloaded online or at checkout counters, are an ideal tool for credit card thieves, drug rings, and even terrorist cells. (See item 7)
- The Associated Press reports the reverse thrusters that should have slowed a Southwest Airlines jetliner before it slid off a runway and into a busy street in Chicago didn't immediately kick in when the pilots tried to deploy them. (See item 10)
- The Boston Globe reports just a week after aviation officials announced changes to improve runway safety at Logan International Airport, the airport recorded its 17th runway incident in the past 14 months, the most of any U.S. airport. (See item 13)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1.

December 09, Associated Press — **Ecoterror probe spurs arrest of woman tied to effort to destroy electricity tower.** Six people were arrested in Oregon, Arizona, Virginia, and New York on ecoterrorism charges in an FBI sweep on both coasts. One of those arrested, Chelsea Dawn Gerlach of Portland, is accused of involvement in the toppling of a Bonneville Power Administration (BPA) tower on December 30, 1999. At the time, the FBI said it appeared to be a case of malicious mischief rather than a Y2K attack. No explosives were used. Support cables were loosened and numerous beer cans were found lying around. The 80−foot−tall tower supported transmission lines that carry surplus BPA energy from the Northwest to Southern California. No loss of service occurred because the load was instantly switched to other lines by computer, and workers re−erected the tower the next day.
Source: http://www.gazettetimes.com/articles/2005/12/09/news/oregon/ friaor00.txt

2. *December 08, Associated Press* — **Energy official urges heating conservation.** Oil and natural gas production in the Gulf Coast area probably will not recover from this year's hurricanes until next summer, Secretary of Energy Sam Bodman said Thursday, December 8, urging conservation as the cost to heat homes is expected to soar this winter. "Even to this day, we have about a third of the natural gas and a third of the oil that is produced in the Gulf of Mexico still shut−in due to the damage that was done," he said. "That's not going to be back up and online, my guess is, until summertime," said Bodman. Short supplies will contribute to high energy prices this heating season, said Bodman, who urged Americans to increase conservation.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/12/08/AR2005120801166.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *December 10, Dallas Morning News (TX)* — **Tanker truck ignites, closes down highway in Texas.** A portion of the President George Bush Turnpike in North Dallas, TX, was shut down in both directions Saturday, December 10, and nearby homes and businesses were evacuated, after a tanker truck carrying between 7,500 and 9,000 gallons of diesel fuel caught fire. The incident occurred shortly after 9 a.m. CST when the driver of the truck noticed that one his back tires had blown out and was on fire. The driver pulled the truck over to the shoulder of the highway and, shortly after, the entire truck erupted in flames. The driver, who was driving for Dupre Transport of Dallas, was not hurt. Dallas Fire and Rescue officials extinguished the blaze about 11 a.m. CST, but traffic on the highway remained closed in both the east and west directions. Fire officials said it may be days before some parts of the road are re−opened.
Source: http://www.dallasnews.com/sharedcontent/dws/news/localnews/stories/121005dnloctanker.162c5ce6.html

4. *December 10, Associated Press* — **Chemical spills in Cape Fear River.** An estimated 1,300 gallons of the chemical paraxylene spilled into the Northeast Cape Fear River but no significant environmental damage is anticipated. The spill occurred late Thursday afternoon, December 8, at an Invista plant in New Hanover County, NC, after a hose split during the transfer of the chemical from a barge to a storage tank, Invista officials said. The transfer process was quickly halted to prevent further release of paraxylene, which is used to make polyester, company officials said. By Friday afternoon, December 9, most of the chemical had been cleaned up, said

Ed Beck, supervisor of the NC Division of Water Quality's Wilmington office. Paraxylene is considered a water pollutant and has the potential to affect birds, plants, fish and other aquatic life. Short−term exposure in humans can cause eye, nose or throat irritation as well as gastrointestinal and neurological effects. Chronic exposure can cause more serious effects, primarily to the central nervous system, and may cause death. No one was injured or became ill because of the incident or cleanup, company spokesperson Erica Taylor said.
Source: http://www.heraldtribune.com/apps/pbcs.dll/article?AID=/2005 1210/APN/512100718

[Return to top]

Defense Industrial Base Sector

5. *December 09, Aerospace Daily & Defense Report* — **Fiscal 2007 defense budget request will align with quadrennial defense review, official says.** The Department of Defense's upcoming fiscal 2007 budget request should align with the results of the ongoing quadrennial defense review (QDR), and may contain some "leading edge" investments springing from QDR strategy, said Christopher "Ryan" Henry, principal deputy undersecretary of defense for policy. The current QDR focuses on Fiscal Year 2008 through Fiscal Year 2013. Henry said the four major themes emerging from the QDR are: the importance of having adaptable forces; the ability of the military to take early measures that prevent problems from evolving into crises and conflicts; unity of effort with services and allies; and balancing military capabilities. The QDR is likely but not guaranteed to specifically mention certain programs, but following the release of the QDR it should be easy to tie its recommendations to the fate of various efforts, Henry said. The Pentagon has announced preliminary cuts in planned defense spending growth of $32 billion from 2007−2011. Roughly 36 percent comes from the Army, with the Navy and the Air Force splitting the rest. The Army, however, will continue receiving the bulk of anticipated supplemental defense spending.
Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/QDR12095.xml

[Return to top]

Banking and Finance Sector

6. *December 09, Associated Press* — **Personal records at university hacked by automated program.** Personal records of those who attended or worked at Idaho State University since 1995 have been compromised. Officials say somebody used an automated computer hacking program to access the personal records, including Social Security numbers, passwords and birthdates. School officials say whoever launched the program may not have even known the information had been accessed. However, school officials and local police have contacted the FBI's cyber crimes unit. The hacking program may have originated in Romania in Eastern Europe. The breach likely occurred in September, but wasn't discovered recently. Idaho State University is located in Pocatello, ID.
Source: http://www.kbcitv.com/x51828.xml?URL=http://10.56.1.26/APWIREFEED/d8ectlfg0.xml&NewsSection=StateHeadlines

7. *December 09, BusinessWeek* — **Law enforcement officials concerned about prepaid gift cards.** Law enforcement officials say prepaid gift cards, many of which can be reloaded online or at checkout counters, are an ideal tool for credit card thieves, drug rings, and even terrorist cells. "It is a great concern to DEA and the FBI because of the terrorist financing angle," says Don Semesky, chief of the office of financial operations at the Drug Enforcement Administration (DEA). There are two kinds of prepaid cards: So−called closed−system cards can be used only at the retailers that issue them, and the newer open−system cards that can be used at almost any retailer. Many can be used as ATM cards and withdraw the amount put on the card anywhere in the world. Most of the open−system cards have MasterCard or Visa logos: Their networks provide the ATM privileges the cards enjoy. "It's the first blending of a bank and nonbank product," says Patrice Motz, a special counsel at Washington law firm Bryan Cave and a former official at the Financial Crimes Enforcement Network of the Treasury Department. That bank/nonbank link is the key to the problem, because the cards have ATM privileges but are not linked to personal bank accounts, which are closely monitored.
   Source: http://moneycentral.msn.com/content/Banking/P137668.asp

8. *December 08, CNNMoney* — **Security concerns over faster method of paying by credit card.** Financial institutions are encouraging customers to use "contactless payment technology," which is a microchip and an antenna implanted in anything from a credit card to a small reader on a key chain. "It's in its infancy, but everyone is going to try to move toward this," said Laura Kaster, an analyst at Sandler O'Niell & Partners. Proponents say it will save time for consumers and could make money for merchants, however, the ease of payment has raised questions as to how easy it would be for thieves to steal the card or information. One analyst said there will be more chances for fraud just by having more card readers in circulation, readers that could be tampered with in order to direct credit card information to a thief and not the bank. "There will be more security holes," said Avivah Litan, security analyst for research company Gartner. "In the end, it increases the risks not decreases them," added Litan. MasterCard, American Express and Visa said all the information sent via the airwaves is encrypted and other monitoring measures are in place, such as cross referencing charges to stores to make sure they accept contactless technology.
   Source: http://money.cnn.com/2005/12/08/pf/blink/index.htm

9. *December 08, Orlando Business Journal (FL)* — **Business, government leaders tackle identity theft issues at summit.** Leaders in law enforcement, government, retail, banking and other fields met Thursday, December 8, during a Florida statewide identity theft summit to discuss the nation's fastest−growing crime. At the second annual Tallahassee summit, hosted by Florida Attorney General Charlie Crist, speakers from both the public and private sectors offered ideas for preventing such theft. A new Florida law cracks down on identity theft by imposing tougher penalties on people who fraudulently use another person's identifying information. The law also requires certain companies that experience identity−related security breaches to notify authorities.
   Source: http://www.bizjournals.com/orlando/stories/2005/12/05/daily3 5.html?from_rss=1

[Return to top]

Transportation and Border Security Sector

10. *December 11, Associated Press* — **NTSB: Crew says jet's reverse thrusters didn't kick in promptly.** The reverse thrusters that should have slowed a Southwest Airlines jetliner before it slid off a runway and into a busy street didn't immediately kick in when the pilots tried to deploy them, federal investigators said Saturday, December 10. after interviewing the crew. The flight attendants said they could tell the Boeing 737 wasn't slowing after it touched down in the snow Thursday evening, December 8, and the pilots said they applied the brakes manually as soon as they realized something was wrong, said Robert Benzon, National Transportation Safety Board (NTSB) investigator in charge. "They all said it was a smooth landing but they could sense a lack of deceleration," Benzon said. The plane, with 98 passengers aboard, slid off a 6,500−foot runway at Midway Airport, through a fence and into street traffic, where it hit two cars and killed a six−year−old boy riding with his family. Ten people, most of them on the ground, were injured. Because of the blowing snow, none of the air traffic controllers actually saw the plane land, but more than 10 cameras have been identified that could provide additional information, including details about the runway conditions, Benzon said
Source: http://www.cnn.com/2005/US/12/11/midway.crash.ap/index.html

11. *December 10, Associated Press* — **Passenger jet crashes in southern Nigeria.** A Nigerian jetliner carrying 110 people, most of them schoolchildren, crashed in stormy weather Saturday, December 10, while landing in the delta oil port of Lagos, and at least 103 people were killed, officials said. Nigerian Civil Aviation Authority spokesperson Sam Adurogboye said early reports indicated that seven people survived the crash of the Sosoliso Airlines' McDonnell Douglas DC−9, which left the capital, Abuja. Frantic family members at the airport said the plane was carrying 75 pupils heading home for the Christmas holidays. Adurogboye said there was stormy weather around the airport at the time of the crash and witnesses said they saw lightning flashes as the plane approached the runway. Saturday's crash was the second Nigeria airplane accident in seven weeks −− raising questions about air safety in Africa's most−populous nation of 130 million people Nigerian airports have come under criticism in recent months following a string of near misses and an incident in which an Air France passenger jet crashed into a herd of cows on the runway at Port Harcourt. International airlines also briefly suspended flights at Lagos' international airport because of holes in the runway.
Source: http://www.usatoday.com/news/world/2005−12−10−nigeria−jet−cr ash_x.htm

12. *December 10, Newsday (NY)* — **New York City airports have safety buffer.** The snow was blowing across the runway at Kennedy Airport last January when the Boeing 747 touched down and kept going. The plane didn't stop at the runway's end, but instead of pitching into the water, the tires of the Polar Air cargo flight sunk into a bed of crushable concrete just beyond the end of the runway, and it came to rest 200 feet short of the water's edge. The jumbo jet wasn't damaged and no one was injured, an example of how a relatively new and simple system used at 14 airports across the country can increase safety at airports where space is at a premium. That safety measure, called Engineered Material Arresting Systems, and is made of blocks of "cellular concrete" −− concrete manufactured with air bubbles in it. The Federal Aviations Administration's (FAA) standards say that a 1,000−foot−long buffer zone should be established at the ends of all runways in case of overruns. But dozens of airports around the country don't have enough space. Some airports without space for buffer zones −− Kennedy and LaGuardia among them −− have received beds of the crushable concrete. The FAA says the material can be used when land is not available because it is already built on, or "where it would be very expensive for the airport sponsor to buy the land off the end of the runway."

Source: http://www.newsday.com/news/nationworld/nation/ny−usskid1210,0,2039944.story?coll=ny−nation−big−pix

13. *December 09, Boston Globe* — **Logan reports another incident on runways.** Just a week after local and federal aviation officials announced changes to improve runway safety at Logan International Airport, the airport recorded its 17th runway incident in the past 14 months, the most of any U.S. airport, federal officials said on Thursday, December 8. Federal Aviation Administration spokesperson Jim Peters said the latest runway incident happened around 4:45 p.m. EST on November 29 when the pilot of a Northwest Airlink commuter jet took off on Logan's runway 22R without permission from the control tower. At the same time, a Continental Airlines 737, which had just landed from Newark with 103 passengers and five crewmembers aboard, was crossing the far end of that runway. The planes were 3,600 feet to 3,800 feet apart horizontally when the Memphis−bound commuter flight with 33 passengers and three crewmembers left the ground, Peters said. Investigators are still trying to determine how close the planes were vertically as the Northwest Airlink plane flew over the Continental jet. The ground radar warning system was working, but did not alert air traffic controllers because it determined the chance of a collision was remote, he said. This incident continues a string of runway incursions that is one of the more perplexing in the nation.
Source: http://www.boston.com/news/local/massachusetts/articles/2005/12/09/logan_reports_another_incident_on_runways/

14. *December 09, Associated Press* — **No injuries reported as Alaska jet jolted by turbulence.** An Alaska Airlines jet was severely jolted by turbulence during a Sitka landing but the airline said no injuries were reported. Flight 70 was arriving Wednesday night, December 7, from Juneau when the plane's right wing dipped suddenly just before the plane leveled and made a bumpy landing. The plane, a 737−400, was later inspected by airline technicians. On board were 44 passengers, two pilots and three flight attendants. A Thursday morning flight from Sitka to Juneau was canceled while the plane was inspected. Amanda Tobin, an Alaska Airlines spokesperson, said she had no immediate word on damage. The airline dispatched workers to the Sitka terminal to comfort passengers. The Federal Aviation Administration logged the incident at 11:23 p.m. local time on Wednesday, noting the plane had undergone "severe" turbulence and landed hard.
Source: http://www.usatoday.com/travel/flights/2005−12−09−alaska−tur bulence_x.htm

15. *December 09, Computerworld* — **Airport pass codes leaked from virus−infected PC.** Pass codes needed to enter secure areas at 16 Japanese airports and one in Guam have appeared on the Internet after a virus infected a computer belonging to a Japan Airlines Corp. (JAL) co−pilot, the airline said on Friday, December 9. The codes, which included those for Tokyo's Narita and Haneda airports and an airport in the U.S. territory of Guam, are typically known to scores of airport workers who need to gain access to areas normally off limits to passengers, said Geoff Tudor, a spokesperson for JAL in Tokyo. Upon learning of the leak, the airports were notified of the need to change the codes. JAL is not planning any disciplinary action against the co−pilot. "He was supposed to have these codes; he hasn't done anything illegal," said Tudor.
Source: http://www.computerworld.com/securitytopics/security/story/0 ,10801,106938,00.html

16.

December 09, Associated Press — **Regional airlines expand while majors suffer.** At a time when the nation's major airlines are being buffeted by skyrocketing fuel costs, heavy competition, and bankruptcies, some regional carriers are posting growing profits and looking to expand. A few regional carriers are struggling or have gone into bankruptcy, following the path of their big airline partners, but others, including Phoenix−based Mesa, Indiana−based Republic, and Utah−based SkyWest, have enjoyed growing profits and significant stock gains. The regional airline sector is growing and profitable thanks to contracts with the major airlines −− which guarantee minimum amounts of revenue and pay some costs −− and because larger airlines are turning over smaller routes to concentrate on those with heavier traffic. Regional carriers usually fly between smaller destinations and major hubs under large airlines' names, logos and ticketing. The large airlines guarantee revenue to the regional carriers, which don't have the expensive union contracts and pension obligations of the major airlines. The regional airlines have deals with the major airlines, which pay their fuel, landing and insurance costs, said Ray Neidl, an analyst with Calyon Securities. That pass−through cost structure buffers them from a lot of the costs that weigh down the larger airlines.
Source: http://www.news−journalonline.com/NewsJournalOnline/Business/Headlines/03BusinessBIZ02120405.htm

17. *December 09, Department of Transportation* — **Department of Transportation's statement concerning Virgin America's application to conduct domestic scheduled air transportation.** On December 8, 2005 the Department of Transportation received Virgin America's application requesting certificate authority to conduct domestic scheduled air transportation. Before any prospective airline can be issued a certificate of authority to operate domestic flights, the Department must confirm the applicant is a U.S. citizen and that it is fit, willing, and able to provide the proposed air transportation. The applicant must provide information concerning its shareholders, key management and technical personnel, historical financial statements, projected operating expenses, and any legal actions against the applicant or its principals. The Department will review the applicant's ownership structure, managerial competence, financing plan, and its disposition toward complying with the rules and regulations governing its proposed operations. The length of the process depends on a number of factors, including the quality of the information provided by the company and any responses received from the public in response to the application.
Virgin America seeks to become a U.S. carrier: Source: http://www.usatoday.com/travel/news/2005−12−08−virgin−americ a_x.htm
Source: http://www.dot.gov/affairs/dot17705.htm

18. *December 09, Department of Transportation* — **Federal Highway Administration offers holiday travel tips to improve safety.** The Federal Highway Administration (FHWA) is encouraging drivers to follow a few simple tips that will help them stay safe during the upcoming holiday travel rush. For real−time updates on traffic, construction areas, lane closures and travel times on interstates and major highways, travelers may take advantage of 511 telephone services now operating in 24 states. A list of 511 telephone services and links to travel Websites with information on traffic jams, weather and road conditions is available on the FHWA Website.
Travel tips: http://www.fhwa.dot.gov/holidaytraveltips.htm
FHWA travel information: http://www.fhwa.dot.gov/trafficinfo/index.htm
Source: http://www.dot.gov/affairs/fhwa1405.htm

[Return to top]

Postal and Shipping Sector

19. *December 08, New England News Service* — **Massachusetts woman charged with stealing post office funds.** A Milford, MA, woman has been charged in U.S. District Court with embezzling U.S. Postal Service (USPS) funds while serving as a supervisor at the Wayland, MA, Post Office since her appointment in October 1998. Sheryl E. Burr of Milford, MA, is accused of using a Postal Service merchant purchase authorization card to obtain goods for her own personal use in addition to those bought to use in supervisory duties. According to USPS Special Agent John Horgan, a number of transactions billed to the USPS by Burr attracted the attention of investigators. They included a vacuum cleaner and accessories valued at $960, three satellite radio systems worth $787, income tax preparation materials priced at $109, and a "Blue Tooth" mobile telephone headset for $63.
Source: http://www.milforddailynews.com/localRegional/view.bg?articl eid=82507

20. *December 08, WTAE−TV (PA)* — **Suspicious package on UPS truck turns out to be computer monitor.** Police, fire, and bomb squad units were called to investigate a suspicious package on a UPS delivery truck in Ross Township, PA, just before noon on Thursday, December 8. Roads were blocked off at Rochester Road and 6th Avenue. Officials said that the words "bomb inside" were written on the box, triggering the alarm. Upon further investigation, officials learned that the package was not dangerous −− it contained a computer monitor.
Source: http://www.thepittsburghchannel.com/news/5492568/detail.html

21. *December 07, ExtremeNano* — **Junk mail beats spam again in 2005.** The Internet continues to take its toll on the U.S. Postal Service (USPS). For the first time in several years, the USPS reported an increase in first−class shipments, albeit a nominal one of one−tenth of one percent. But that's the first time in several years that the USPS didn't report a sharp drop in first−class mail. The government's figures last year showed that Americans sent 103.7 billion pieces of first−class mail in 2001 and only 97.9 billion pieces in 2004, about a six percent drop. In 2005, that number closed out just shy of 98.1 billion. The traditional kind of consumer first class traffic −− consisting of bills, bill payments, and personal correspondence −− plummeted 3.8 percent, to 45.9 billion pieces. USPS officials attribute that loss to electronic payments. "There is a pretty healthy erosion of single−piece mail...People are finding an alternative way to pay," said James P. Cochrane, manager of package services for the USPS. Cochrane said USPS officials say that bill pay online is likely a trend that won't be reversed. Other factors causing the decay of first−class single−piece mail include personal e−mail and e−mail's ability to handle much larger electronic attachments than a few years ago.
Source: http://www.extremenano.com/print_article/Junk+Mail+Beats+Spam+Again+in+05/167005.aspx

[Return to top]

Agriculture Sector

22. *December 09, USAgNet* — **Pork producers warned of the threat borne by feral pigs.** The Pork Checkoff is urging producers to be on look−out for feral pigs. Feral pigs can cause extensive damage to property, crops, and are a threat to the health of the national swine herd. According to the U.S. Department of Agriculture (USDA), there are an estimated four million wild pigs distributed across 39 states in the U.S. The population and distribution of these feral pigs has expanded in the last decade and wild pigs have been sighted and hunted in some of the country's largest pork producing states including Iowa, North Carolina, Oklahoma, and Texas. Wild pigs are carriers of external parasites and of diseases important to the pork industry such as brucellosis, pseudorabies (PRV), classical swine fever, foot−and−mouth disease, African swine fever, porcine reproduction and respiratory syndrome (PRSS), swine influenza virus, and leptospirosis. According to USDA data, feral pig populations that are serologically−positive to brucellosis have been found in 14 states. Pseudorabies has been confirmed in feral pig populations in at least 11 states. In 2003, feral pigs sampled in South Carolina were found serologically positive to the H1 subtype of the swine influenza virus and serologically positive to PRRS. Pork producers can protect their herds from contact with wild pigs though strict biosecurity including perimeter fencing.
Source: http://www.usagnet.com/story−national.cfm?Id=1230&yr=2005

23. *December 09, Star Tribune (WY)* — **Wasting disease expands in deer.** Chronic wasting disease (CWD) researchers have found higher−than−expected infection rates among fawns and two−year−old white−tailed deer in central Wyoming. The most alarming finding was infection rates of up to 80 percent in two−year−old white−tailed deer in a hunting area near Glenrock that has an overall wasting disease prevalence rate of 31 percent, according to researchers from the University of Wyoming's (UW) School of Veterinary Sciences. UW graduate student David Edmunds is two years into his master's project, focused on CWD in hunt area 65 miles west of Glenrock. Each March, he captures 30 new fawns and also recaptures older deer he has previously tagged. Area 65 has ranged in the 22 to 30 percentile in recent years. Preliminary data from Edmunds show that: fawns have a 10 percent infection rate, yearlings have a 26 percent infection rate, and two−year−olds have an 80 percent infection rate. "We were surprised at the number of fawns who are infected," said Edmunds' adviser, Todd Cornish. What that indicates, he said, is that deer can become infected with the fatal brain disease at an early age.
CWD information: http://www.cwd−info.org/
Source: http://www.jacksonholestartrib.com/articles/2005/12/09/news/wyoming/296423b20b3208e6872570d20006e814.txt

[Return to top]

Food Sector

24. *December 09, Bloomberg* — **Beef producers may take years to restore beef sales to Japan.** U.S. beef producers may take years to recover lost exports to Japan, once their biggest overseas buyer, after the country allows them to resume shipments. Companies may need that much time because cattle supplies are relatively low and Japanese consumers are leery of mad−cow disease, the reason for a two−year prohibition on U.S. beef imports. The ban, imposed after the disease was found in a cow in Washington state, may be lifted as soon as Monday, December 12, the Asahi newspaper said on Tuesday, December 6. Sales will return slowly because U.S.

slaughterhouses are unable to quickly find cattle that meet the conditions Japan will impose on imports, said Sam Rovit, chief executive of Colorado−based Swift, the third−largest U.S. producer. Japanese consumers also are eating less beef, so producers need to win back that business, he said. "It may be three to four years before we return to levels seen before the market was closed," said Mark Klein, a spokesperson for Cargill Meat Solutions in Minnesota. The company, a unit of Cargill Inc., is the second−largest U.S. beef processor.
Source: http://www.bloomberg.com/apps/news?pid=10000101&sid=ahpKkjxa6_MY&refer=japan

25. *December 08, Associated Press* — **Salmonella found in raw milk.** State health officials are warning the public about tainted raw milk from an Arizona dairy. Inspectors from the Arizona Department of Health Services found Salmonella bacteria in a sample of unpasteurized raw milk taken from a retailer in Yavapai County. The milk was produced by Meadowayne Dairy of Colorado City. The levels of Salmonella in the sample couldn't be measured, so it isn't known if there was enough bacteria to cause illness.
Source: http://www.tucsoncitizen.com/breakingnews/120805AZ_Tained_Mi lk

[Return to top]

Water Sector

26. *December 09, New Orleans Times−Picayune (LA)* — **East New Orleans water now safe to drink.** The water is safe to drink in eastern New Orleans, LA, according to the Sewerage and Water Board. According to the board, the Louisiana Department of Health and Hospitals on Thursday, December 8, lifted the boil−water advisory for all of eastern New Orleans, including Venetian Isles, but not including the lower Ninth Ward or ZIP Code 70117 east of the Industrial Canal. The tap water is now safe for drinking, cooking, and bathing, according to the board. Although water in New Orleans, west of the Industrial Canal, was deemed safe on October 6, the Sewerage and Water Board had to fight numerous leaks and low water pressure throughout much of eastern New Orleans. Work on the lines is continuing throughout the city, the board said.
Source: http://www.nola.com/news/t−p/metro/index.ssf?/base/news−12/1134113245319820.xml

[Return to top]

Public Health Sector

27. *December 09, Reuters* — **Bird flu kills Thai boy.** Bird flu killed a young Thai boy, Asia's 70th victim of the deadly virus, authorities said on Friday, December 9. The death of the 5−year−old boy from the central province of Nakhon Nayok, 70 miles from Bangkok, took Thailand's bird flu death toll to 14 out of 22 known cases since the virus swept through large parts of Asia in late 2003. He was the second Thai killed by the H5N1 virus since bird flu erupted anew in the country in October, when a 48−year−old man died. It was not yet certain how the boy caught the virus, which usually strikes those in close contact with infected fowl or their droppings, senior health officials said. The boy, who died in hospital on Wednesday, December 7, was not

known to have had direct contact with chickens, health officials said. "We believe that the boy contracted the virus from his surroundings because, although his family does not raise chickens, there are chickens raised in his neighborhood," said Thawat Suntrajarn, head of the Health Ministry's Disease Control Department.
Source: http://today.reuters.com/news/newsarticle.aspx?type=worldNews&storyid=2005−12−09T070634Z_01_KNE914514_RTRUKOC_0_US−BIRDFLU−THAILAND.xml&rpc=22

28. *December 09, Newhouse News Service* — **Virtual emergency room trains doctors.** The State University of New York (SUNY) Upstate Medical University has a new virtual ER, where the patients are computerized mannequins −− known as human patient simulators. They speak, moan, bleed, drool, urinate, blink their eyes, and perform many other lifelike functions. Complex internal wiring and software allow each dummy to have a heart attack, break into a sweat from a bioterrorism attack, or feign just about any other injury or illness. The emergency medicine training center is equipped with oxygen, patient monitors, ventilators, a defibrillator and all the other equipment normally found in a real emergency room. Human patient simulators are becoming an increasingly popular teaching tool for doctors, nurses, and paramedics nationwide. The military uses them to train for mass casualties. "If they make a mistake on the mannequin, it's not hurting a patient," said Richard Cherry, the center's technical director who orchestrates the emergency scenarios. The simulators allow the medical school to create situations that can't be scheduled in the ER. Residents are not told in advance what's wrong with the patient. They begin with the limited amount of information they can glean from the patient's chart. Residents respond to the exercises as if they were the real thing.
Source: http://www.sunherald.com/mld/thesunherald/news/world/13365699.htm

29. *December 09, Xinhua (China)* — **Russian lab confirms deadly strain of bird flu in Ukraine.** The bird flu virus found in Ukraine has been confirmed as the deadly strain of H5N1, a Russian agriculture official said Friday, December 9. "This is so−called Asian strain H5N1 that poses a potential threat to man," Russian chief agriculture inspector Sergei Dankvert told the Itar−Tass news agency, referring to the virus found in Ukraine and sent to the All−Russia Research Institute of Animal Protection for testing. Ukraine is also waiting for results of laboratory tests in Britain next week. Ukraine recorded its first case of bird flu Saturday, December 3, and the disease has spread rapidly across parts of the Crimea peninsula in the past week. Ukrainian officials said Thursday, December 8, the bird flu virus had been confirmed in eight residential areas of the Crimea, where more than 30,000 fowl were already culled. By Wednesday, December 7, the country's Emergency Situations Ministry had seized about 28,000 birds in house−to−house checks in villages in a sealed−off exclusion zone.
Source: http://news.xinhuanet.com/english/2005−12/09/content_3900700.htm

30. *December 08, Reuters* — **Bird flu seen posing $675 billion threat to U.S. economy.** A human outbreak of bird flu in the United States could deal a $675 billion blow to the economy, U.S. Senate Majority Leader Bill Frist said on Thursday, December 8, citing a new study by the Congressional Budget Office (CBO). Frist said the study assumed a 2.5 percent mortality rate, that 30 percent of the population would be infected and that employees would miss three weeks of work. The economic loss estimated by the study would amount to a five percent reduction in gross domestic product, he said. The H5N1 avian influenza virus is spreading steadily among poultry, pushing westward out of Asia into Europe. Health officials fear it will mutate, become

easily transmitted among humans and spread rapidly around the world, killing tens of millions of people. The virus is known to have infected just 135 people since 2003 but has killed more than half of them.
CBO Report: http://www.cbo.gov/ftpdocs/69xx/doc6946/12−08−BirdFlu.pdf
Source: http://today.reuters.com/investing/financeArticle.aspx?type=governmentFilingsNews&storyID=URI:urn:newsml:reuters.com:20051208:MTFH34654_2005−12−08_18−06−00_N08320332:1

31. *December 08, University of Pittsburgh* — **Mathematics used for discerning immune response to infectious diseases, vaccine development.** The National Institutes of Health (NIH) has awarded the University of Pittsburgh School of Medicine a five−year, $9.1 million contract to develop sophisticated mathematical models for investigating how the immune system responds to specific pathogens. The contract establishes Pitt as an Immune Modeling Center, one of four supported by the NIH's National Institute of Allergy and Infectious Diseases (NIAID), and takes advantage of Pitt's existing collaborations with Carnegie Mellon University and the University of Michigan. The Immune Modeling Center will focus on understanding the innate, or natural, and adaptive immune responses to influenza A virus, Mycobacterium tuberculosis, which causes TB, and Francisella tularensis, the bacterium responsible for tularemia. Since each of these organisms enters the body via the lung, the investigators will study the specific immune cells recruited to the lung and identify the particular genes expressed and the molecules produced in response to infection. A combination of mathematical and animal models will be employed to test different vaccine and therapeutic strategies, including a novel approach that aims to enhance immune response through certain proteins called cytokines. The other institutions receiving NIAID contracts to support Immune Modeling Centers are Duke University, the University of Rochester, and Mount Sinai School of Medicine.
Source: http://newsbureau.upmc.com/TX/ImmuneModelingCenter.htm

32. *December 08, Associated Press* — **U.S. had just 37 cases of measles in 2004.** The U.S. had just 37 cases of measles in 2004, the smallest number in more than 90 years of record keeping, the government said Thursday, December. Nearly all of the cases originated abroad, with 14 occurring in U.S. residents who traveled to other nations, 13 in foreigners who brought the disease to the U.S., and six in people infected by those two groups. In the decade before a measles vaccine became available in 1963, more than 500,000 measles cases and about 450 measles deaths occurred in the U.S. each year. The U.S. vaccination rate against measles is now over 90 percent.
Measles information: http://www.cdc.gov/ncidod/diseases/submenus/sub_measles.htm
Source: http://www.cbsnews.com/stories/2005/12/08/ap/health/mainD8EC 6VKG0.shtml

33. *December 06, Agency for Healthcare Research and Quality* — **Video shows clinicians how to treat children exposed to chemicals used in bioterrorist attacks.** Tuesday, December 6, the U.S. Department of Health and Human Services' Agency for Healthcare Research and Quality (AHRQ) released The Decontamination of Children: Preparedness and Response for Hospital Emergency Departments, a 27−minute video that trains emergency responders and hospital emergency department staff to decontaminate children after being exposed to hazardous chemicals during a bioterrorist attack or other disaster. This video provides a step−by−step demonstration of the decontamination process in real time and trains clinicians about the

nuances of treating infants and children, who require special attention during decontamination procedures. Produced for AHRQ's Bioterrorism Preparedness Research Program, the video outlines key differences between decontaminating children and adults; provides an overview for constructing portable and permanent decontamination showers and designating hot and cold zones; and provides steps to establishing and maintaining pediatric decontamination capacity in a hospital emergency department. A free, single copy of the video −− available in DVD or VHS format −− may be ordered by calling 1−800−358−9295 or by sending an E−mail to ahrqpubs@ahrq.gov.
Source: http://www.ahrq.gov/news/press/pr2005/deconvidpr.htm

[Return to top]

Government Sector

34. *December 10, Associated Press* — **Man charged for illegal possession of TNT threatens Minnesota state government building.** A man who allegedly threatened to set off TNT at the Bureau of Criminal Apprehension headquarters in St. Paul, MN, was charged Friday, December 9, with illegal possession of explosives. Authorities say Michael John Hagemann showed an informant who was working with deputies a brick in his possession labeled with the words "TNT" and "explosive." Sheriff Bob Fletcher said, "There were some hearsay comments made by the defendant to other people that he was considering targeting law enforcement agencies −− one mentioned by name was the Bureau of Criminal Apprehension." The sheriff said Hagemann was not charged with making terroristic threats because there wasn't enough evidence. The case will be turned over to federal authorities.
Source: http://wcco.com/topstories/local_story_343183900.html

[Return to top]

Emergency Services Sector

35. *December 09, Associated Press* — **Charleston Harbor braces for disaster drill.** Beginning Monday, December 12, 300 personnel from more than 40 local, state and federal agencies in South Carolina will take part in a two−day drill simulating terrorists attacking Charleston, SC, with a weapon−of−mass−destruction. To the public, the drill may look like the real thing with people portraying armed terrorists, helicopters flying around, emergency lights flashing and mock casualties. The drill will continue through Tuesday, December 13. Officials are not saying exactly how the mock attack will be staged so that the emergency responders will have to react as though it were a real event. Local police and rescue agencies in South Carolina will participate in this week's drill as will the Coast Guard, the Domestic Nuclear Detection Office, the U.S. Department of Justice's Project SeaHawk, the Federal Bureau of Investigation and the Department of Health and Environmental Control. SeaHawk is the pilot port security effort helping to protect Charleston from terrorist threats. Initiated almost three years ago, it involves almost 50 local, state and federal agencies working together to assess threats that could enter the country through Charleston.
Source: http://www.thestate.com/mld/thestate/13370677.htm

36. *December 09, Government Technology* — **Department of Homeland Security to distribute commercial IT to first responders.** The Department of Homeland Security (DHS) is preparing to distribute geospatial information−sharing software and other commercial IT to local jurisdictions through its Commercial Equipment Direct Assistance Program (CEDAP). CEDAP is operated by the DHS' Office of State and Local Government Coordination and Preparedness to help smaller communities that have not received direct federal homeland security grants. Earlier this year, the department awarded technology valued at $8 million to 697 jurisdictions under the program. The program provides the technology, along with installation and technical assistance, directly to eligible jurisdictions rather than through a grant program. The offerings include personal protective equipment, rescue tools, thermal imaging, chemical and biological sensors, and risk management software. Some IT being distributed by CEDAP include: geographic information system software and training; Coplink information−sharing and investigative lead−generating products for law enforcement; i2 Analyst's Notebook, which is visualization software for investigative analysis; PEAC−WMD (Palmtop Emergency Action for Chemicals−Weapons of Mass Destruction) decision support and incident command software for first responders. The CEDAP program receives advice and guidance from the International Association of Chiefs of Police, the National Sheriffs Association and the Fraternal Order of Police.
Source: http://www.washingtontechnology.com/news/1_1/daily_news/2755 3−1.html

37. *December 09, Associated Press* — **For states, Katrina erasing distinctions between emergency preparedness, homeland security.** Whether they're concerned about terrorism or earthquakes, state lawmakers gathered for a national conference say that the government shortcomings exposed by Hurricane Katrina demand a new look at disaster preparedness across the country. Renewed talk of evacuation drills, backup communications, and stresses on U.S. health care networks dominated discussion Thursday, December 8, at the fall meeting of the National Conference of State Legislatures. The threat of terrorism has been a driving force since September 11, but hurricane Katrina made clear that years of security work at all levels of government hasn't been enough. Most lawmakers discussed what their states must do to prepare for a comparable disaster. "In any substantial emergency you better not expect the federal government to do anything soon. You better have your own resources," said state representative Phil Barnhardt (D−OR). The problem is that leaders haven't consistently devoted time or resources to get ready for a hypothetical worst−case scenario. Some lawmakers talked of revisiting emergency evacuation plans. Others discussed the still unresolved inability for different emergency response agencies to communicate on the same radio equipment.
Source: http://www.dailysouthtown.com/southtown/dsnews/095nd1.htm

38. *December 08, Associated Press* — **"Throwaway" camera designed to help police.** Police officers stepping into hostage standoffs and other dicey situations now have something new to throw into the mix −− a baseball−sized camera that can be hurled from afar, survive the landing and wirelessly relay video and audio back to base for two hours. The camera, known as EyeBall, weighs less than a pound and is protected by a rugged rubber and polyurethane housing. That allows it to be thrown through windows or bounced off walls. When it comes to a rest, the ball stabilizes itself, then begins transmitting footage and sound up to 200 yards away. Other methods for remotely grabbing audio and video in dangerous operations often require getting close to the action, a potentially lethal step. Police can expect to pay $4,800 for two EyeBalls, whose batteries require recharging after about two hours of use, and the

corresponding video monitoring equipment.
Source: http://www.nytimes.com/aponline/technology/AP−TechBits.html

[Return to top]

Information Technology and Telecommunications Sector

39. *December 18, Tech Web News* — **Sites installing spyware via zero−day Internet Explorer bug.** A still−unpatched Internet Explorer vulnerability that's been used by attackers since late November to compromise Windows PCs is now being used by large numbers of malicious Websites to plant spyware and adware, a security company claimed Thursday, December 8. San Diego−based Websense said in an alert that it's detected thousands of sites connecting to a main malicious URL that's "actively exploiting this vulnerability to execute malicious code," according to the warning. All it takes is a visit to one of the sites with Internet Explorer running on Windows 98, Windows Me, Windows 2000, or Windows XP, to compromise a computer, the warning noted. A bogus warning that the machine is infected with spyware appears and a so−called "spyware cleaning" application launches. That application then prompts the user to enter a credit card number. What's actually installed, however, is real spyware, which then connects to a URL in the .biz domain to download and run more than 10 other programs that install without the user's consent. According to Websense, the .biz domain Website is real, but has been compromised by hackers. It's hosted in the U.S., and is currently still online.
Source: http://www.techweb.com/wire/security/174907332;jsessionid=WRE35TOIAV2AUQSNDBECKH0CJUMEKJVN

40. *December 09, VNU Net* — **First Firefox 1.5 exploit made public.** Security experts at Packet Storm have published proof−of−concept code that exploits an unpatched flaw in the Firefox 1.5 browser, making the application vulnerable to a denial of service attack. The code marks the first publicly disclosed security vulnerability in Firefox 1.5 since the version became available in late November. The published code will add a large entry to the 'history.dat' file of the browser, causing the application to freeze or crash the next time it is launched. Users can fix the problem by manually erasing the file. Another option is to change the browser setting to disable the saving of history data by setting the days of saved history to zero or increasing the privacy control. While the proof−of−concept code is relatively harmless, the flaw could be exploited to install malware, according to John Bambenek, a researcher with the University of Illinois at Urbana−Champaign and a volunteer at the SANS Internet Storm Center. "Presumably, if the topic was more tightly crafted than in the proof−of−concept code, a more malicious attack could be crafted that would install malware on the machine with the extra step of being reinstalled after each restart of Firefox," Bambenek wrote.
Source: http://www.vnunet.com/vnunet/news/2147377/firefox−expoit−mad e−public

41. *December 09, eWeek* — **eBay pulls bidding for Microsoft Excel vulnerability.** An unknown security researcher chose a novel way to issue a warning for a code execution flaw in Excel −− posting it for sale on eBay. But the auction was pulled late Thursday, December 8, after discussions between Microsoft and eBay Inc. When the auction was squashed, the bidding had reached $53 and had attracted 19 offers. A spokesperson for Microsoft confirmed that the eBay listing was indeed a legitimate security flaw in Excel. In the listing, posted by a seller named "fearwall," the issue is described as a zero−day vulnerability that was discovered on Tuesday,

December 6, 2005, and reported to Microsoft. The seller openly taunts the software giant, poking fun at the company's delays in providing fixes for known security bugs. "It can be assumed that no patch addressing this vulnerability will be available within the next few months. So, since I was unable to find any use for this by−product of Microsoft developers, it is now available for you at the low starting price of $0.01 (a fair value estimation for any Microsoft product)," the listing read.
Source: http://www.eweek.com/article2/0,1895,1899697,00.asp

42. *December 08, Security Focus* — **Microsoft December advance notification unspecified security vulnerabilities.** Microsoft has stated the update for these unspecified vulnerabilities will be released on December 13, 2005. These updates may require users to reboot their computers after installation.
Source: http://www.securityfocus.com/bid/15782/references

43. *December 08, Security Focus* — **Microsoft Excel unspecified memory corruption vulnerability.** An unconfirmed vulnerability has been reported to exist in Microsoft Excel. The vulnerability was announced on eBay. The discoverer is offering to sell the vulnerability details. According to the auction description, it is possible to have a large value passed to "msvcrt.memmove()" through data fields in an Excel .xls file. The discoverer has claimed that code execution is possible.
Source: http://www.securityfocus.com/bid/15780/references

44. *December 08, Security Focus* — **Mozilla Firefox large history file denial of service vulnerability.** Mozilla Firefox is reportedly prone to a remote denial of service vulnerability. This issue presents itself when the browser handles a large 'history.dat' file. An attacker may trigger this issue by enticing a user to visit a malicious Website and supplying excessive data to be stored in the affected file. This may cause a denial of service condition due to resource exhaustion.
Source: http://www.securityfocus.com/bid/15773/references

45. *December 08, Tech Web News* — **Microsoft to beef up Internet Explorer 7 security.** Microsoft is changing Internet Explorer (IE) 7's security zones in a bid to create a more attack−resistant browser, according to a public blog entry written by three developers at the software giant. Like its predecessors, IE 7 enforces security policies by clumping sites into four security categories, or zones, dubbed Internet, Intranet, Trusted Sites, and Restricted Sites. Typically, the Intranet zone comes with fewer restrictions than the Internet zone. In the past, however, attackers have sometimes managed to fool IE into treating an outside site as in one of the less−secure zones, known as a "zone−spoofing attack." To prevent some of these attacks, IE 7 will instead treat all sites as being in the more−secure Internet zone, unless the PC is really part of a managed network (such as is often the case in a corporate environment). "This change effectively removes the attack surface of the intranet zone for home PC users," wrote Vishu Gupta, Rob Franco and Venkat Kudulur, on the trio's "IEblog".
Source: http://www.techweb.com/wire/security/174906971;jsessionid=WRE35TOIAV2AUQSNDBECKH0CJUMEKJVN

46. *December 08, IDG News Service* — **U.S. calls on Japan to further open telecom sector.** The U.S. called on Japan to increase regulatory transparency in the telecommunications and

information technology sectors on Wednesday, December 7, as it delivered its annual set of government reform recommendations. The proposals were presented by Wendy Cutler, U.S. Trade Representative (USTR) for Japan, Korea, and APEC Affairs to Japanese government officials as a bilateral meeting began in Seattle, WA. They were made under the U.S.−Japan Regulatory Reform and Competition Policy Initiative, which was started in 2001 to promote economic ties between the two countries. Included on the list was the shifting of telecommunications regulatory functions to an independent agency away from ministerial control. The U.S. also called on Japan to increase public participation in regulatory and policy decisions, ensure termination rates charged by mobile carriers are reasonable, ensure spectrum management policies and practices are more transparently administered, and conclude a mutual recognition agreement for equipment certification. This last issue would simplify certification of mobile handsets capable of operating on both the Japanese and U.S. cellular standards and is expected to be agreed this week.
Annual Reform Recommendations from the U.S. to the Government of Japan:
http://www.ustr.gov/assets/World_Regions/North_Asia/Japan/Regulatory_Reform_Initiative/asset_upload_file792_8516.pdf
Source: http://www.networkworld.com/news/2005/120805−japan−telecom.h tml

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of a cross domain violation in Internet Explorer. This may allow a script in one domain to access web content in a different domain.Web browsers should adhere to the "Same Origin Policy", which prevents documents or scripts loaded from one origin from getting or setting properties of a document from a different origin. Internet Explorer does not follow this policy when importing CSS documents. For more information please see URL: http://www.mozilla.org/projects/security/components/same−ori gin.html

If the cross domain violation in Internet Explorer occurs on a system that has Google Desktop Search (GDS) installed, then an attacker may be able to search for private data, execute programs, or execute arbitrary code on this vulnerable system. Google has modified its web pages to prevent exploitation of GDS through this particular vulnerability in Internet Explorer. The cross domain violation vulnerability in Internet Explorer is still present, however. Although there is limited information concerning this vulnerability, US−CERT encourages users to disable Active scripting to prevent exploitation. For more information please review URL: http://www.cert.org/tech_tips/malicious_code_FAQ.html#ie566

Users can also refer to the Microsoft Security Response Center Blog for some additional information on this vulnerability affecting Internet Explorer. For more information please see:

http://blogs.technet.com/msrc/archive/2005/12/07/415740.aspx x

Automatic Update Functionality in Sober.X Worm US−CERT is aware of functionality that could allow the mass mailing worm known as "W32/Sober.X" to automatically update itself. W32/Sober.X is a bi−lingual (English and German) mass mailing worm that utilizes its own SMTP engine to propagate. The W32/Sober.X worm began propagating on November 15, 2005 and will attempt to update itself on or around January 5, 2006. Systems that have already been compromised by the W32/Sober.X worm are expected to receive this update. Once the update is received, the W32/Sober.X worm may execute code that reduces the security protection of vulnerable systems. US−CERT strongly recommends that users and administrators implement the following general protection measures:

Install anti−virus software, and keep its virus signature files up to date.

Do not follow unsolicited web links or execute attachments received in email messages, even if sent by a known and trusted source.

Keep up to date on patches and fixes for your operating system.

For more information please review the US−CERT Computer Virus Resources at URL: http://www.us−cert.gov/other_sources/viruses.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 445 (microsoft−ds), 80 (www), 27015 (halflife), 49889 (−−−), 4142 (oidocsvc), 25 (smtp), 135 (epmap), 139 (netbios−ssn) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

47. *December 09, Associated Press* — **Hostage standoff forces evacuation of Salvation Army center.** A man held a woman hostage for six hours Friday, December 9, forcing the evacuation of a Salvation Army center in Rochester, NY, police said. The standoff in a downtown building ended with his surrender. No one was hurt. The suspect, who was not immediately identified, told police that he had a weapon and was holding a women hostage, said police spokesperson Joseph Dominick. Police negotiators eventually persuaded him to give up. Another person, sitting up on a stretcher, was also taken away. Police did not reveal whether the man was armed.
Source: http://www.newsday.com/news/local/wire/newyork/ny−bc−ny−−salvationarmy−sta1209dec09,0,1039541.story?coll=ny−region−apnew york

48. *December 09, CBS−5* — **Hoax causes Wyoming school to go under lockdown.** There were tense times at a Cheyenne, WY, junior high school Friday, December 9, after police received a false report that a gunman had taken five students hostage. Police and swat team members responded to Carey Junior High School at 11:00 a.m. MST when someone used the school's payphone to falsely report the incident. The school was immediately put into lockdown while officials searched the school. Nothing out of the ordinary was found.
Source: http://www.kgwn.tv/home/headlines/2073657.html

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.